

# Linux サーバの立ち上げと運用に必要な知識の習得

町原 秀夫（第一技術室）、坂口 義輝、田畑 功（第二技術室）  
白井 治彦、松山 幸雄、水野 広治、吉田 祥造（第三技術室）

## 1. はじめに

技術部には現在、メールサービスとアクセス制限された Web サービスを行う情報サーバ（以下、Kozml と略）があるが、耐用年数等で後継マシンの整備と技術継承が課題となっている。一方、近年では汎用的なパソコンにフリーソフトの PC-UNIX をインストールしたネットワークサーバが広く利用されており、本格的な UNIX マシンの機能が AT 互換機などで個人レベルでも手軽に構築することが可能となっている。

そこで、本研修では、新たに DOS/V パソコンを組立て、フリーで利用できる Debian GNU Linux sarge 版（以下、Debian と略）を用いたメールサーバの構築と運用管理技術の研修を行なった。総合情報処理センター（以下、センターと略）の実習室には Debian が導入されている端末が相当数設置されているため、専任教員の講義と実習を通して Debian の初歩、パッケージ管理ツール、セキュリティについての学習を行うとともに、組立てたパソコンを用いて Debian のインストールと設定を行った。最終段階ではメールサーバとしての設定を終え、問題なく稼働することを確認した。

表 1 研修用パソコンの仕様

Mother Board	ASUS P4G800-V VGA・LAN・SOUND内蔵
CPU	Intel Pentium4 2.80GHz
メモリ	256MB×2枚 PC2700
ハードディスク	Maxtor ATA100 40GB×2台
DVDマルチドライブ	GSA-4120B LG
フロッピードライブ	3.5 inch 2mode
電源	350W（ケースに内蔵）

## 2. 研修内容

### 2.1 組立てパソコンの仕様

Debian を導入したサーバを立ち上げるには一定の能力を持ったパソコンが必須となる。表 1 に組立てパソコン（以下、kenshu と略）のパーツと仕様を示す。

本格的なサーバを構築するためには Raid によるミラーリングが必要となるが、予算の制約からこの機能は設定していない。誤操作によるシステム停止からマシンを保護するために、パワースイッチと直列にトグルスイッチをケースの後部に取り付けた。ハブは、kozml が 100/10Mbps の自動切替えに未対応のため、ポートモード設定スイッチを装備したスイッチングハブを使用した。

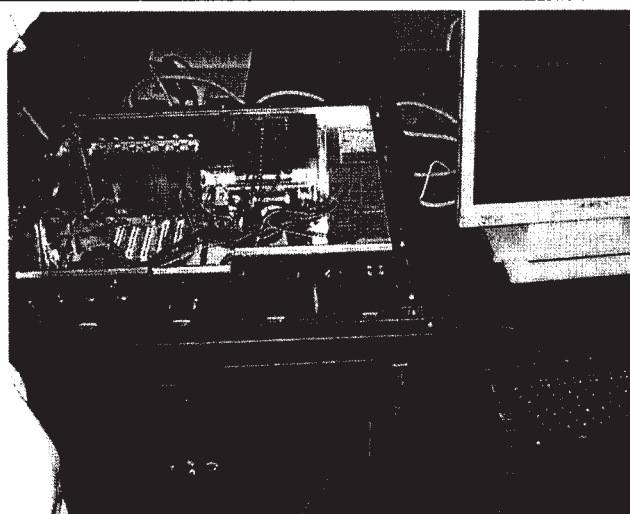


写真 1. 組立風景

## 2.2 センター実習

### 2.2.1 Debian のインストール

インストールする Debian はテスト版ではあるが、機能拡張された Serge を使用した。センター実習では最初に、ネットワーク、Linux とハードウェアに関する基礎知識の講義を受けた。そして準備されたマニュアルを基に、設置されているパソコンを使用し、OS インストール、パッケージ管理ツール、ファイアーウォールなどの使用法、設定を学んだ。インストール方法は、福井大学総合情報センターが Debian のミラーサイトになっているため、利便性を考慮してネットワークを利用してのインストールを行った。

### 2.2.2 パッケージ管理ツール

インストーラを終了させた後にソフトウェアの追加・更新・削除を行う場合にはパッケージ管理ツールを使用する。Debian のパッケージにはソースパッケージ（プログラムのソースコードとその管理情報を一つのファイルにまとめたもの）とバイナリパッケージ（各種アプリケーションソフトのパッケージ）の 2 種があり、管理ツールでは主として後者のパッケージを管理する。このツールにはコマンドライン版(`apt-get`, `dpkg` など)、コンソール版(`aptitude`, `dselect` など)、GUI 版(`gnome-appt` など)があり、研修では日常のシステムメンテナンスで主に使用する以下のコマンドについて実習した。

`apt-get update` (パッケージサーバーから最新のリストを取得)

`apt-get upgrade` (取得したリストを元に現在のシステムを更新)

`aptitude` (フルスクリーンのコンソール画面で、追加・削除するパッケージを選択・実行)

この他、現在では `aptitude` に取って代わられた `dselect` や、依存関係を見捨てて個別にパッケージをインストールする `dpkg` などがあり、テキストを通じてこれらの使用方法を学習した。

### 2.2.3 iptables によるセキュリティ対策の学習

センターでの最後の実習では、ホストのネットワークセキュリティ対策を目的としている `iptables` についての実習を行った。これは、ホストとネットワーク間の通信を制御して安全性を高めるもので、フィルタリング機能や NAT (アドレス変更) 機能など、パラメータの設定により柔軟にフィルタリングが構築できる。

`iptables` は、「filter」、「nat」、「mangle」(パケットパラメータの書き換え) の機能ごとにテーブルがあり、各テーブルはチェーンから構成されている。チェーンとは、パケットなどに対する具体的な制御処理を記述した `iptables` のコマンドであるルールが順に並んだリストである。また、チェーンにはユーザ定義と組み込み済みチェーンがあり、組み込みチェーンには適用するパケットの種類により共通な名前が付いている。主なものに、自ホスト宛パケットが対象の `INPUT` チェイン、自ホストからネットワークへのパケットが対象の `OUTPUT` チェイン、自ホストを通過するパケットが対象の `FORWARD` チェインなどがある。これらのチェーンのルールによりホストのアクセス制御が可能となる。このルールを記述する複数の `iptables` コマンドでは、ホストに対するアクセスルールに従い、条件を記述した順に指定したフレームやパケットなどの内容とチェックされ、その結果によりアクセス可否の処理が実行される。

実習では、`iptables` のインストールからルールの設定、実行、確認などの方法を学習した。具体的には、`telnet` サーバにおけるパケットフィルタリング構築を例に、サブネット内からのアクセス

は許可し、サブネット外からのアクセスに対してはログを取り、更に、組織内からのアクセスにはメッセージ付きで拒否する内容の設定を行った。これらのルールはコマンドにて設定・追加するため再起動時には再度設定が必要となる。そこで、起動時にフィルタリングが適用されるように、ルールのコマンドを記述したファイルを作成し、起動時に実行できるように設定した。なお、iptables はカーネルと密着して機能しており iptables の機能を組み込むためにカーネルの再構築も行った。

kenshu に対しても、同じように telnet におけるパケット制限の設定を行い kozm1 とのネットワーク通信を利用して動作の確認を行った。

ルールの内容は、kozml が接続しているサブネットから kenshu への telnet アクセスのみを許可し、それ以外からの telnet アクセスに対しては記録を残す設定とした(図-1)。但し今回は iptables の動作確認を目的としているため、kenshu システムを考慮した具体的なフィルタリング処理は設定していない。

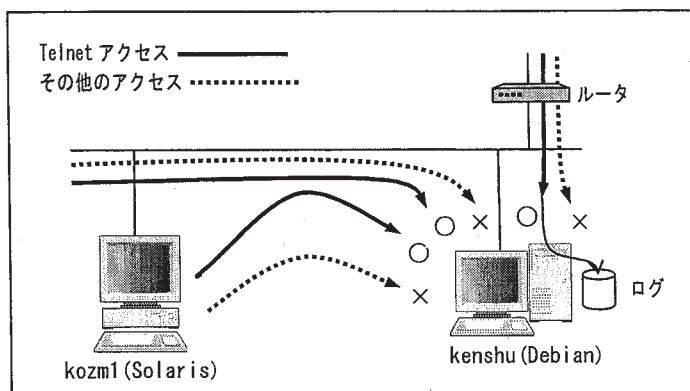


図-1 iptables による制御 (kenshu)

### 2.3 メールサーバ

メールサーバは、図-2のようにクライアント(A)からの要求に基づいて電子メールを送信するSMTP(Simple Mail Transfer Protocol)サーバと、届いたメールを保管してクライアント(B)からの照会があったときに引き渡すPOP(Post Office Protocol)サーバから構成されている。

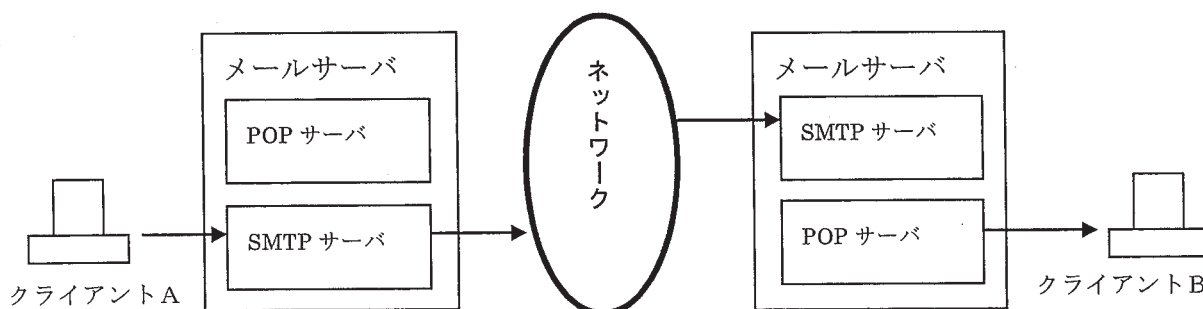


図-2 メールの流れ

#### 2.3.1 SMTP サーバ

メールの送信は送信側と受信側でSMTPというプロトコルにより、メールアドレスを頼りに最終目的地までメールを中継配送するMTA(Message Transfer Agent)によって行われる。MTAには、sendmail, postfix, qmail などがあり、Debianには最初からexim4がインストールされているが、本研修では機能的にも柔軟性がありメジャーなsendmailを使用した。

#### 2.3.2 sendmail

インストールはデフォルトでインストール済みのexim4を削除してから行った。sendmailの設定は、どのような表現形式をどう解釈するかというルールセットを定義したsendmail.cfファイルで行うが、これは非常に複雑で読み書きをするのに困難な文法になっているため、一般的な利用形態のみのルールセットを生成するツール(CF, m4)を用いて作成する。ディストリビュータよりダウンロードしたsendmail-8.13.3にはm4マクロプロセッサによるdebian用の定義ファイル

sendmail.mc ファイルが用意されているので、使用環境に応じた追加変更を行った。ここでは、「access」、「mailertable」、「local-host-names」の各ファイルを作成し、kozml 間でのメールの送受信の動作確認を行った。

2.3.3 POP サーバ

MTA によって届き保管したメールは、クライアントからメールの取得要求を受け、パスワード認証を行い配信される。本研修では一般に用いられている qpopper を使用した。qpopper は apop(Authenticate post Office Protocol) にも対応しており、暗号化するパスワードをPOPサーバコンソールから登録することにより、パスワード認証時のパスワードの漏洩を防ぐことができる。本研修では、パソコン上の Almail を使用して動作を確認した。

3. おわりに

本研修では、センターでの講義と設置されているパソコンを使用した実習により、限られた研修時間内で効率よく OS の学習を行うことができた。また、Debian がテスト版で頻繁に更新されるため、実習毎にアップデートが不可欠であった。

Windows マシンの操作しか知らない技術者からサーバ管理を業務としている技術者まで広く募集して行ったため、新しい OS についての理解度には差が生じたが、情報系の人がリードすることで、研修用に用意したパソコンをメールサーバとして立ち上げることが出来た。

時間の関係上、Web サーバの構築には至らず、また、運用に必要な知識も十分ではないため、今後もこの種の研修を継続する必要がある。

4. 謝辞

センターの専任教員である田中光也先生には4回にわたるセンター実習の講師を快諾いただき、なおかつ多くのテキストを準備していただきました。ここに深く感謝いたします。

[参考文献]

1) Debian GNU/Linux Expert sarge 対応 ; 技術評論社 平成 16 年 9 月発行

[研修日誌]

専門研修実施日程

9月 8日	専門研修打合せ	購入パーツ、消耗品、IPアドレス申請
9月24日	第一回センター実習	Debianのインストール
10月14日	第二回センター実習	Debianのインストール
10月21日	パソコンの組立てとDebianのインストール	
10月28日	Debian のインストール	
11月 4日	第三回センター実習	パッケージ管理ツールの使い方
11月11日	Debian のインストール作業	
11月25日	ネットワーク接続作業	情報コンセント, kenshu, kozmlをハブに接続
12月 8日	テキストによる輪読	Debian GNU/Linux Expert <sup>1)</sup>
2月16日	日本語環境の導入と設定	
3月 8日	第四回センター実習	iptablesの使い方
3月17日	メールソフトsendmailの導入、設定と動作確認	
3月24日	ハードディスク増設 & kenshuの再設定	
3月29日	メールソフトqpopperの導入と動作確認および総括	